AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

Target Accounts as further described in Attachments A-1, A-2, A-3, and A-4

Case No. MJ19-072

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

Target Accounts as further described in Attachments A-1, A-2, A-3, and A-4, which are attached hereto and incorporated herein by this reference.

located in the Northern District of California, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachments B-1, B-2, B-3, and B-4 for a list of information to be disclosed, which are attached hereto and incorporated herein by this reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
Title 18, U.S.C. § 371; 1349	Conspiracy;
Title 18, U.S.C. § 1028; 1029	Aggravated Identity Theft; Access Device Fraud;
Title 18, U.S.C. § 1030; 1343	Computer Fraud; Wire Fraud

The application is based on these facts:

See attached Affidavit of Special Agent Joel Martini

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Joel Martini, Special Agent FBI
Printed name and title

Sworn to before me and signed in my presence.

Date: 02/21/2019

Judge's signature

City and state: Seattle, Washington

United States Magistrate Judge Mary Alice Theiler
Printed name and title

AFFIDAVIT

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, Joel Martini, being first duly sworn, depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), currently assigned to the Seattle Field Office, and have been so employed for approximately 2 years. I am assigned to the Cyber squad where I primarily investigate computer intrusions and other Cybercrimes. My experience as an FBI Agent includes the investigation of cases involving the use of computers and the Internet to commit crimes. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, Cybercrimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment. I have received advanced training in the acquisition and analysis of digital evidence (both network and host based), responding to computer intrusions and other incidents. I currently hold a Bachelor's of Science in Information Systems from Corban University.

2. Prior to my employment as a Special Agent, I worked as a Computer Forensic Examiner for the FBI for approximately 5 years. As part of that employment, I became familiar with the design and operations of various electronic devices, networks, and websites, including technology described herein.

3. I make this affidavit in support of an application for a search warrant for information associated with certain accounts (collectively, "**TARGET ACCOUNTS**") that are stored at premises controlled by an electronic communications service and/or remote computer service provider ("Provider"), referenced below. The information to be searched is described in the following paragraphs and in Attachments A, which are incorporated herein.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require the following:

a. **Twitter, Inc.** ("Twitter"), located at 1355 Market Street, Suite 900, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-1, pertaining to the following account(s), identified in Attachment A-1:

i. **User ID: 178776029**, also known as "**@ryanrocks462**" ("**SUBJECT ACCOUNT 1**")

ii. **User ID: 715225783**, also known as "**@ryanrocks562**" ("**SUBJECT ACCOUNT 2**")

b. **Discord, Inc.** ("Discord"), located at 444 De Haro St., Suite 200, San Francisco, California, to disclose to the government copies of the information, including the content of communications, further described in Section I of Attachment B-2, pertaining to the following account(s), identified in Attachment A-2:

i. **User ID: 451537312900317201**, also known as username "**ryanrocks462#8138**" ("**SUBJECT ACCOUNT 3**")

ii. **Server ID: 419619233622654986**, also known as "**Ryan's Underground Hangout**" ("**SUBJECT DISCORD SERVER**")

c. **Apple, Inc.** ("Apple"), located at One Apple Park Way, Cupertino, California, to disclose to the government copies of the information, including the content, further described in Section I of Attachment B-3, pertaining to the following account(s), identified in Attachment A-3:

i. **Apple ID: 1710515926**, associated with **ryanrocks462@icloud.com** ("**SUBJECT ACCOUNT 7**")

d. **Google, LLC** ("Google"), located at 1600 Amphitheatre Parkway, Mountain View, California, to disclose to the government copies of the information, including the content, further described in Section I of Attachment B-4, pertaining to the following account(s), identified in Attachment A-4:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

i. **Account ID: 279578011651**, associated with **ryanrocks562@gmail.com** ("**SUBJECT ACCOUNT 8**").

Upon receipt of the information described in Section I of Attachments B, government-authorized persons will review that information to locate the items described in Section II of Attachments B. This warrant is requested in connection with an on-going investigation in this district by the Seattle Field Office of the Federal Bureau of Investigation (FBI).

4. As discussed herein, the FBI is conducting an investigation into an unauthorized network intrusion and data breach of Nintendo Co., Ltd, and Nintendo of America (collectively, "Nintendo"), for which there is probable cause to conclude was committed by RYAN HERNANDEZ (DOB: 01/24/1999), also known as "Ryan West" and by the online alias "RyanRocks," a resident of Palmdale, California, and the user of each of the **TARGET ACCOUNTS**.

5. The facts set forth in this Affidavit are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement personnel; review of documents and records related to this investigation; communications with others who have personal knowledge of the events and circumstances described herein; and information gained through my training and experience. Because this Affidavit is submitted for the limited purpose of establishing probable cause in support of the application for a search warrant, it does not set forth each and every fact that I or others have learned during the course of this investigation.

6. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud) have been committed by RYAN HERNANDEZ, as described below, as well as perhaps other unknown persons. There is also probable cause to search the information described in Attachments A for evidence, instrumentalities, contraband or fruits of these crimes, as described in Attachments B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

SUMMARY OF PROBABLE CAUSE

A. Background

7. The FBI is conducting an investigation into a suspected hacking scheme, having received information from Nintendo regarding unauthorized access to Nintendo computer systems and the subsequent theft and dissemination of confidential and proprietary data. The suspected threat actor was identified as RYAN HERNANDEZ, an individual previously known to Nintendo and to the FBI for prior similar conduct. HERNANDEZ is the user of each of the **TARGET ACCOUNTS**.

8. Nintendo is a consumer electronics and video game company. Nintendo Co., Ltd, is headquartered in Japan, and its North American subsidiary, Nintendo of America, is located in Redmond, Washington. Nintendo has manufactured a variety of home and handheld game consoles, such as the Wii U, 3DS, and the Switch, and developed multiple popular video game franchises, such as Mario, The Legend of Zelda, Pokémon, Animal Crossing, and Splatoon, among others.

9. RYAN HERNANDEZ (DOB: 01/24/1999) resides at 40520 Aster Pl, Palmdale, California ("TARGET RESIDENCE"), with his parents Ruben and Sheila Hernandez.

10. For some time, from approximately December 2015 until late November 2018, the static home IP address[1] for HERNANDEZ at the TARGET RESIDENCE was 172.248.227.193. According to records obtained from Charter Communications in July 2017, the service provider for this IP address (172.248.227.193), the account was activated in December 2015 in the name of "Ruben Hernandez" (HERNANDEZ's father) at the Palmdale, California TARGET RESIDENCE:[2]

---

[1] An Internet Protocol address (or simply "IP address") is a unique numeric address used by devices, such as computers, on the Internet. Every device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses.

[2] Investigators have requested, but not yet received, updated records from Charter Communications related to this IP address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Target Details	172.248.227.193, 9/9/2016 12:01:00 AM, GMT, 0
Subscriber Name:	RUBEN HERNANDEZ
Subscriber Address:	40520 ASTER PL, PALMDALE, CA 93551-2508
Service Type - RR HSD	Activate Date: 12/14/2015 Deactivate Date: Still Active
User Name or Features:	RHERNANDEZ56051@roadrunner.com
Phone number:	(661)526-4285, (661)361-3386
Advanced Subscriber Info	
Account Number:	8448200050282192
Equipment Details	
MAC:	d405983403e2
Other Details	
Other Information:	IP Lease Information: First seen: 1/14/2016 1:06:52 PM Through 6/10/2017 1:26:52 AM

On about September 15, 2018, HERNANDEZ (ryanrocks462) (**User ID: 451537312900317201 (SUBJECT ACCOUNT 3)**) also posted his home IP address (172.248.227.193) on his Discord server, "Ryan's Underground Hangout" (**Server ID: 419619233622654986 (SUBJECT DISCORD SERVER)**):

11. In late November 2018, the static home IP address for HERNANDEZ at the TARGET RESIDENCE changed to 76.232.194.142. According to records obtained from AT&T, the service provider for this new IP address (76.232.194.142), the account was established on November 21, 2018, registered to "Ruben Hernandez" at the Palmdale, California TARGET RESIDENCE:

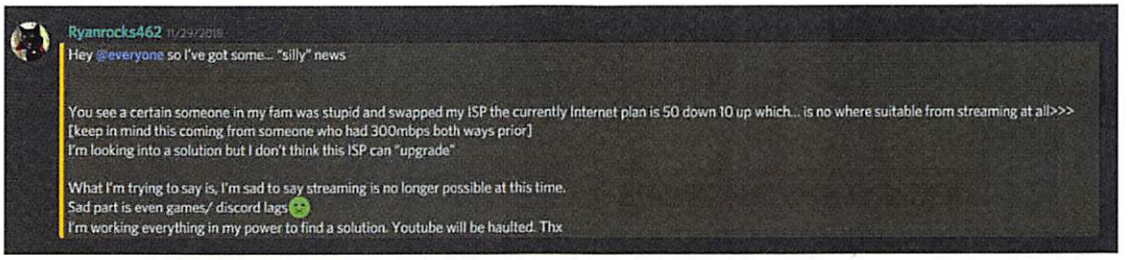
> Subscriber Information

Primary Contact Information		Account Information	Open
Contact Name:	RUBEN HERNANDEZ	Account Id:	290237662
CBR:	661-361-3386	Account Name:	RUBEN HERNANDEZ
ALT CBR:	661-361-2982	Member Id:	rubenhernandez7337@att.net
Preferred Email:	rhernandez5630...	Established:	11/21/2018
Authenticated By:	Passcode / QA	Sub Type:	Consumer
		Business Type:	
		Network Type:	FTTN-BP
		Billing:	AT&T
		Bill Cycle:	2
		Bill Media:	Paper
		AutoPay:	No
		Bill Language:	English

As discussed below, HERNANDEZ expressly discussed his family's change of Internet service provider (ISP) on his Discord server **(SUBJECT DISCORD SERVER)**. More specifically, on about November 29, 2018, HERNANDEZ (ryanrocks462) **(SUBJECT ACCOUNT 3)** expressed displeasure about a family member changing to a different service

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

provider with reduced download and upload speed, which caused him problems:

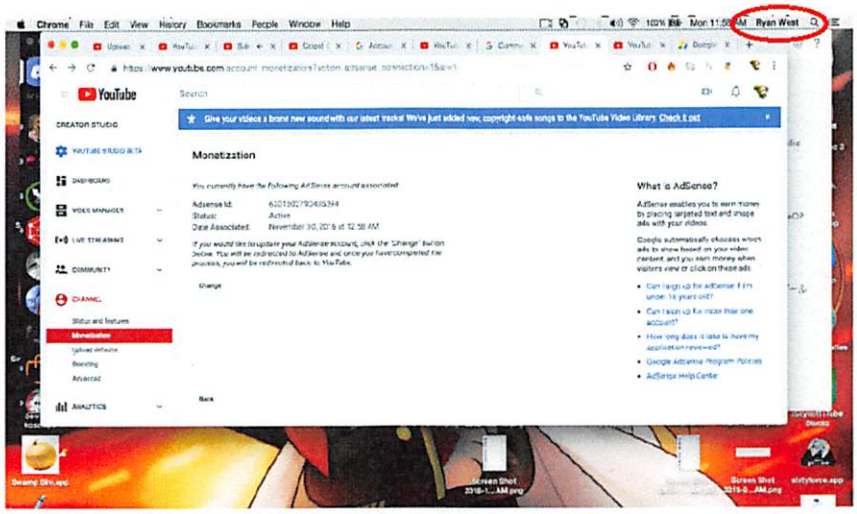


Based on the circumstances, investigators believe HERNANDEZ's post on Discord was reference to his father (Ruben) and the switch to AT&T (from Charter Communications, the provider of IP address 172.248.227.193).

12. RYAN HERNANDEZ uses aliases, most commonly "Ryan West," and various online monikers incorporating "RyanRocks." For instance, HERNANDEZ maintains a Facebook account under the username "ryan.west.462." According to records obtained from Facebook, that account was registered in May 2011 under the name Ryan West, using ryanrocks562@yahoo.com (SUBJECT ACCOUNT 5). The associated payment information includes a Visa credit card ending in -8048, and an American Express card ending in -1723, both in the name of RYAN HERNANDEZ, as well as a PayPal account associated with email ryanrocks562@yahoo.com (SUBJECT ACCOUNT 5).

13. Furthermore, on various screenshots posted by HERNANDEZ (ryanrocks462) **(SUBJECT ACCOUNT 3)** on his Discord server, "Ryan's Underground Hangout" **(SUBJECT DISCORD SERVER)**, the username of "Ryan West" regularly appears, as set forth in the example below:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



B. Summary of RYAN HERNANDEZ's History of Targeting Nintendo

14. As described below, RYAN HERNANDEZ is an individual known to Nintendo who has repeatedly targeted Nintendo and its products.

15. In 2016, HERNANDEZ registered for Nintendo developer access, including, among other things, accepting the terms of a non-disclosure agreement governing the use and disclosure of information. HERNANDEZ then accessed confidential and proprietary information, including material for the Wii U console and Nintendo 3DS system, through Nintendo's developer sites. HERNANDEZ then, in violation of the terms of the non-disclosure agreement and various laws, publicly posted and disclosed such information. Such disclosures of confidential and proprietary information increase the risk of piracy of Nintendo products, among other harms caused to Nintendo.

16. Nintendo, through its representative, contacted HERNANDEZ demanding he cease and desist such conduct. In about September 2016, HERNANDEZ, then a minor, and his parents agreed that HERNANDEZ would cease such activities and cease use of Nintendo's developer sites and confidential and proprietary information.

17. HERNANDEZ thereafter engaged in hacking activity targeting Nintendo and stole confidential and proprietary information, which led to a criminal referral and law enforcement contact. As part of that prior conduct, HERNANDEZ used some of the same online accounts and the same IP address as the current intrusion under investigation.

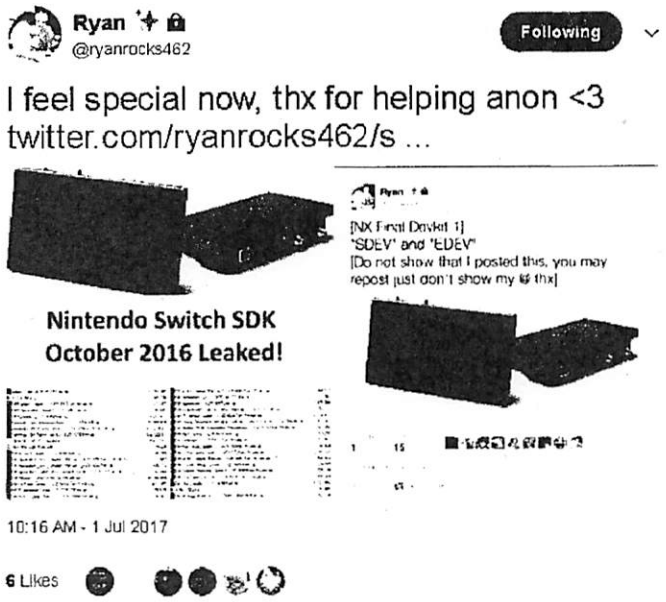
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

18. More specifically, in about October 2016, a user on Nintendo's online Developer Portal successfully persuaded a Nintendo employee to respond to a help request posted on a Nintendo online forum. Upon clicking on a link posted by the threat actor, the Nintendo employee's Developer Portal credentials were hijacked and obtained by the originating user. The threat actor then used the stolen account credentials to upload malware onto the site, which logged the tokens of legitimate users logging onto the site, and later to gain administrator access to the Developer Portal and download proprietary Nintendo data.

19. Nintendo launched an internal investigation into the incident, remediated the intrusion, and identified the malicious user as RYAN HERNANDEZ of Palmdale, California. This identification was made in part by matching the IP address (172.248.227.193) used for the attack with the IP address legitimately used by HERNANDEZ on the Nintendo network. Further, Nintendo noticed that some of the stolen data was appearing on a Twitter account with the username **@ryanrocks462 (SUBJECT ACCOUNT 1)**.

20. In March 2017, Nintendo contacted FBI Seattle regarding the above attack. FBI Seattle opened an investigation and confirmed through legal process that the IP address (172.248.227.193) used to hack Nintendo's network was registered to "Ruben Hernandez," in Palmdale, California (TARGET RESIDENCE), where RYAN HERNANDEZ also resided. Nintendo also provided FBI with copies of Twitter posts from user **@ryanrocks462 (SUBJECT ACCOUNT 1)** implying responsibility for leaking Nintendo information. For instance, in July 2017, Twitter user **@ryanrocks462 (SUBJECT ACCOUNT 1)** appeared to take credit for the leak of data related to the Nintendo Switch SDK, while thanking "anon" for assistance:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



21. On about October 25, 2017, FBI agents (including this affiant) contacted and interviewed RYAN HERNANDEZ at his Palmdale, California residence (TARGET RESIDENCE).[3] Also present were HERNANDEZ's parents, Ruben and Sheila Hernandez. HERNANDEZ confirmed that he used Twitter account **@ryanrocks462 (SUBJECT ACCOUNT 1)** but initially claimed that his posts about hacking Nintendo were simply jokes. After initially denying involvement in the Nintendo hack, HERNANDEZ later acknowledged accessing the Nintendo Developer Portal but claimed he did so at the direction of an unknown anonymous Twitter user who had since deleted his/her account. HERNANDEZ also claimed to have deleted any Nintendo data. At the conclusion of the interview, HERNANDEZ promised to stop any further malicious activity against Nintendo and indicated an understanding of potential consequences of future criminal activity.

C. Summary of Investigation and use of TARGET ACCOUNTS

22. In October 2018, Nintendo first contacted FBI Seattle to report further intrusion activity, which it attributed to RYAN HERNANDEZ. Nintendo observed a threat

[3] During the interview, RYAN HERNANDEZ responded to investigators' questions predominantly in writing and through gestures. According to his father, HERNANDEZ was seeing specialists for developmental difficulties.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

actor at the same IP address (172.248.227.193) previously identified as associated with HERNANDEZ's Palmdale, California residence (TARGET RESIDENCE) using an unauthorized authentication certificate to access various internal Nintendo development tools and unreleased game titles, among other things. Nintendo provided the FBI with various identifiers and accounts associated with HERNANDEZ, including the **TARGET ACCOUNTS**. According to Nintendo, its internal examination of its network and remediation efforts ultimately uncovered HERNANDEZ's unauthorized access to multiple Nintendo servers dedicated to various stages of product development and distribution, dating back to at least June 2018. Some of the impacted servers are located in the Western District of Washington.

23. In January 2019, Nintendo representatives provided additional details about Nintendo's ongoing remediation of HERNANDEZ's intrusion and its prior dealings with HERNANDEZ, including the 2016 conduct, discussed above. Nintendo communicated locating unauthorized network access by 172.248.227.193 and more recently 76.232.194.142, which was deterimined to be HERNANDEZ's more recent home IP address. According to Nintendo, to date, it had located evidence of HERNANDEZ's unauthorized access to at least four server groups. For instance, one of the server groups related to a staging environment for the Nintendo eShop, which was used for pre-production testing. In June 2018, HERNANDEZ's home IP address accessed the server(s), which required use of a legitimate certificate.[4] The actor requested pre-release information and downloaded data, including development tools and retail titles Splatoon 2 and Minecraft. Similarly, in June 2018, an IP address belonging to HERNANDEZ accessed the device authentication server group using an illegitimate certificate. Beginning in July 2018, HERNANDEZ's IP address accessed the server group that managed content for retail kiosks, including advertising material and game demos. Nintendo suspected that the certificates

[4] According to Nintendo, it observed other unauthorized actors using the same credentials, which led it to believe that the particular compromised credentials had been shared on some online forum or group.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

required from such access were possibly obtained from an application extracted from the previously compromised staging environment server group.

24. As part of its referral, Nintendo provided the FBI with information it had gathered about HERNANDEZ and his activity relating to Nintendo and its products.[5] As conveyed by Nintendo, RYAN HERNANDEZ openly discussed Nintendo and Nintendo products and his theft of Nintendo property through various online accounts.

25. RYAN HERNANDEZ maintains a large number and wide variety of accounts at various service providers, including, but not limited to, the **TARGET ACCOUNTS**. For instance, investigators have identified several email accounts believed to be used by HERNANDEZ, including: ryanrocks462@yahoo.com ("SUBJECT ACCOUNT 4"), ryanrocks562@yahoo.com ("SUBJECT ACCOUNT 5"), ryanrocks463@yahoo.com ("SUBJECT ACCOUNT 6"), ryanrocks462@gmail.com, **ryanrocks562@gmail.com (SUBJECT ACCOUNT 8)**, **ryanrocks462@icloud.com (SUBJECT ACCOUNT 7)**, and ryanrocks462@outlook.com.

26. It appears that RYAN HERNANDEZ frequently has used his Yahoo (Oath Holdings, Inc. ("Oath")) accounts, ryanrocks462@yahoo.com (SUBJECT ACCOUNT 4), ryanrocks562@yahoo.com (SUBJECT ACCOUNT 5), and ryanrocks463@yahoo.com (SUBJECT ACCOUNT 6), particularly to register other email and social media accounts. Each of these Yahoo accounts is registered using HERNANDEZ's known alias "Ryan West." According to records obtained from Oath, account ryanrocks462@yahoo.com (SUBJECT ACCOUNT 4) was registered in 2009, and is in the name "Mr Ryan West" with an alternative email address of ryanrocks463@yahoo.com (SUBJECT ACCOUNT 6):

[5] Nintendo retains a third-party company to assist in monitoring and investigating threat activity and threat actors.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Login Name:	ryanrocks462
GUID:	RVPGZ7RYWQY4GFOBP2J5FUIIJAA
Properties Used:	Answers Flickr Mail
Yahoo Mail Name:	ryanrocks462@yahoo.com
Alternate Communication Channels:	ryanrocks463@yahoo.com *Verified* 1 6613613779 *Verified*
Registration IP address:	75.40.64.184
Account Created (reg):	Wed Oct 14 01:02:22 2009 GMT
Other Identities:	ryanrocks462 (Yahoo! Mail)
Full Name	Mr Ryan West

Account ryanrocks562@yahoo.com (SUBJECT ACCOUNT 5) was registered in 2011, in the name "Ryan West" with an alternative email address of ryanrocks462@yahoo.com (SUBJECT ACCOUNT 4):

Login Name:	ryanrocks562
GUID:	V2ZEQBTL6CNEM2DHIS5SSOB4SE
Properties Used:	Mail Groups
Yahoo Mail Name:	ryanrocks562@yahoo.com
Alternate Communication Channels:	ryanrocks462@yahoo.com *Verified* 1 6613613779 *Verified*
Registration IP address:	184.72.15.185
Account Created (reg):	Tue May 17 06:40:07 2011 GMT
Other Identities:	ryanrocks562 (Yahoo! Mail)
Full Name	Ryan West

Email ryanrocks463@yahoo.com (SUBJECT ACCOUNT 6) was registered in 2012, in the name "Ryan West":

Login Name:	ryanrocks463
GUID:	QJ5CXVGAPVUOO6WSNGOHPGPR6A
Properties Used:	Mail
Yahoo Mail Name:	ryanrocks463@yahoo.com
Alternate Communication Channels:	1 6613613779 *Verified*
Registration IP address:	75.22.49.170
Account Created (reg):	Sat Apr 14 04:33:17 2012 GMT
Other Identities:	ryanrocks463 (Yahoo! Mail)
Full Name	Ryan West

The three Yahoo accounts are all associated with the same phone number, 661-361-3779.

27. As of December 26, 2018 (the date of Oath's production), the most recent log on for each of these "ryanrocks" Yahoo accounts occurred on December 11, 2018, which leads investigators to believe the accounts remain active.

Discord TARGET ACCOUNTS

28. Nintendo provided the FBI with screenshots and summaries of various posts by Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) on HERNANDEZ's Discord server called "Ryan's Underground Hangout" (**Server ID: 419619233622654986 (SUBJECT DISCORD SERVER)**). As discussed below, Discord basically enables users to create chatrooms (called "servers") where users can communicate through posts and/or direct messages as well as through voice or video chat. HERNANDEZ's **SUBJECT DISCORD SERVER** also had various "channels," which are akin to topic-specific message boards or chats, which included such names as #nintendo-switch-keys, #switch-title-keys, #hacky-talk, #splatoon-2-talk, #splatoon-1-shit, among several others.

29. The FBI confirmed that RYAN HERNANDEZ is Discord user ryanrocks462 (**User ID: 451537312900317201 (SUBJECT ACCOUNT 3)**), the operator of "Ryan's Underground Hangout" **(SUBJECT DISCORD SERVER)**. According to records obtained from Discord, HERNANDEZ's account ryanrocks462 **(SUBJECT ACCOUNT 3)** was registered on May 31, 2018, from HERNANDEZ's home IP address (172.248.227.193), using email ryanrocks463@yahoo.com (SUBJECT ACCOUNT 6):

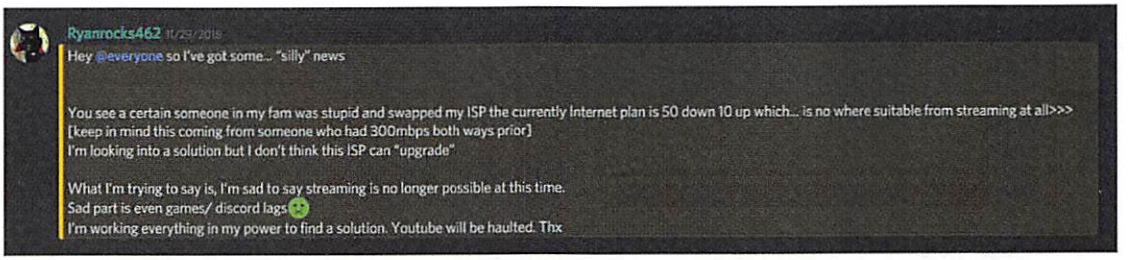
User ID:	451537312900317201
Username:	Ryanrocks462#8138
Email:	ryanrocks463@yahoo.com
Registration Time (UTC):	2018-05-31 00:08:05
Registration IP:	172.248.227.193

Additionally, Discord IP log records confirmed that HERNANDEZ's account was accessed regularly from HERNANDEZ's home IP address (172.248.227.193), i.e., from the TARGET RESIDENCE and from the same IP address used to access Nintendo's network, between August 18, 2018 (the first date of the logs provided) until November 28, 2018. Thereafter, Discord account ryanrocks462 **(SUBJECT ACCOUNT 3)** was regularly accessed through the new IP address (76.232.194.142) for the TARGET RESIDENCE.

30. As noted above, according to records obtained from AT&T, the account

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

associated with this IP address (76.232.194.142) for HERNANDEZ's Palmdale, California TARGET RESIDENCE was established on November 21, 2018, registered to "Ruben Hernandez." Moreover, as noted above, according to screenshots provided by Nintendo, in late November 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** posted on Discord **(SUBJECT DISCORD SERVER)** about his frustration of a family member changing to a different Internet service provider, which prompted him to halt streaming and his YouTube account:



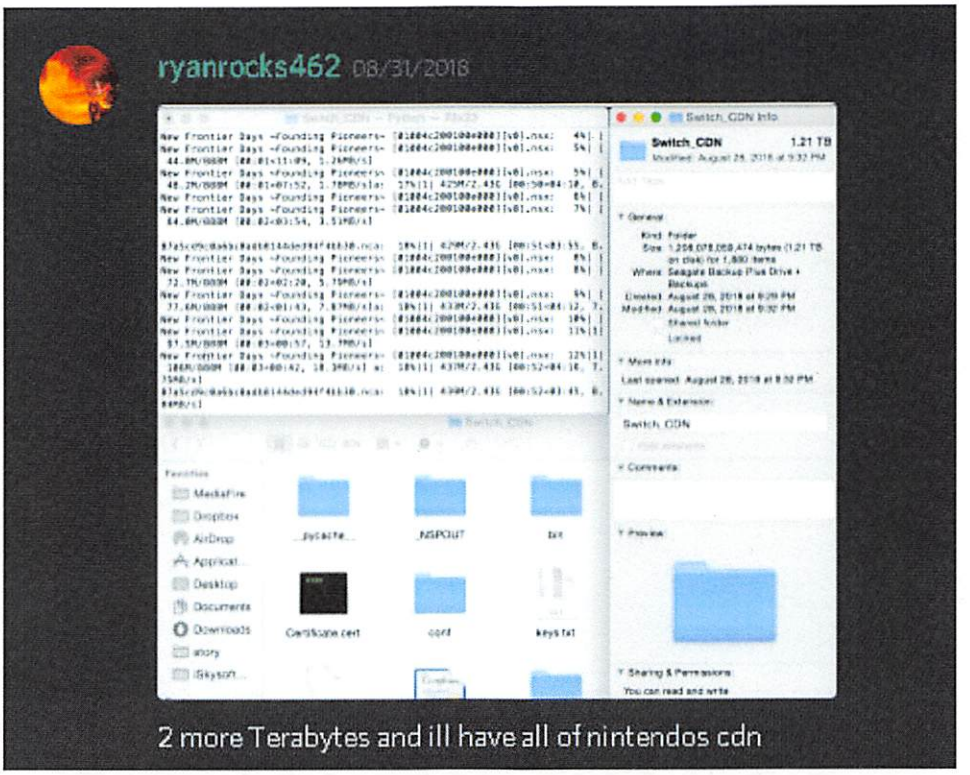
On December 3, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** posted that the issues were resolved and included a link to his new YouTube channel, stating that his next stream would likely be "splatfest," which I recognize as a reference to the Nintendo Splatoon game:

31. Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted on Ryan's Underground Hangout" **(SUBJECT DISCORD SERVER)** numerous messages suggesting he was engaged in hacking activity and had unauthorized access to files and information pertaining to Nintendo products.[6] Below are several examples:

[6] All of the sample screenshots and summaries of Discord postings described herein were provided to the FBI by Nintendo and occurred on Ryan's Underground Hangout" **(SUBJECT DISCORD SERVER)**. It is believed that HERNANDEZ participates on other servers as well. For instance, in October 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted an

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

a. Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) claimed to have access to Nintendo servers and was actively downloading content, specifically related to the Nintendo Switch. For instance, on August 28, 2018, ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted a screenshot of what appears to be a file folder titled "Switch_CDN" along with the message: "2 more Terabytes and ill have all of nintendos cdn":[7]



On about September 3, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted a similar image of the "Switch_CDN" file folder with the message: "just the jap titles to go oml":[8]

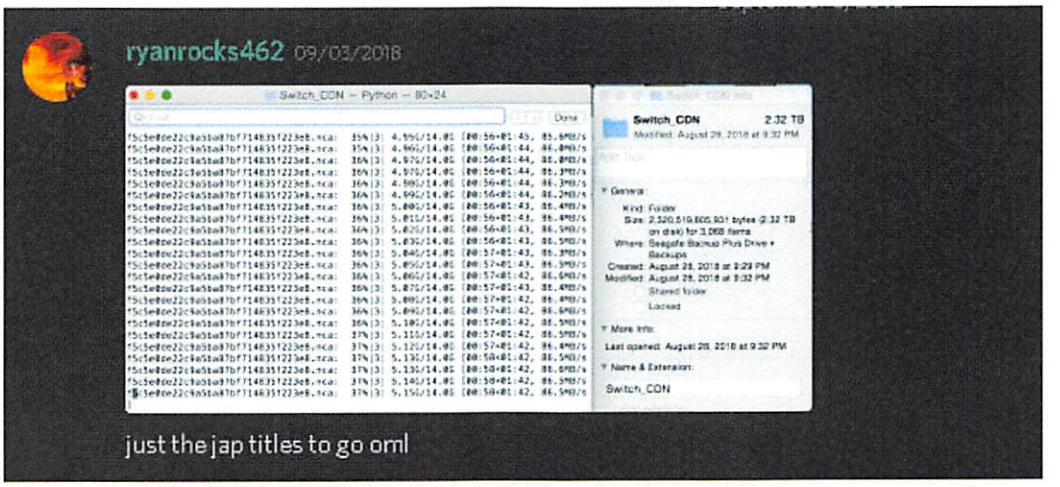
---

invitation to another Discord server called "WarezNX," which is believed to also relate to Nintendo products.

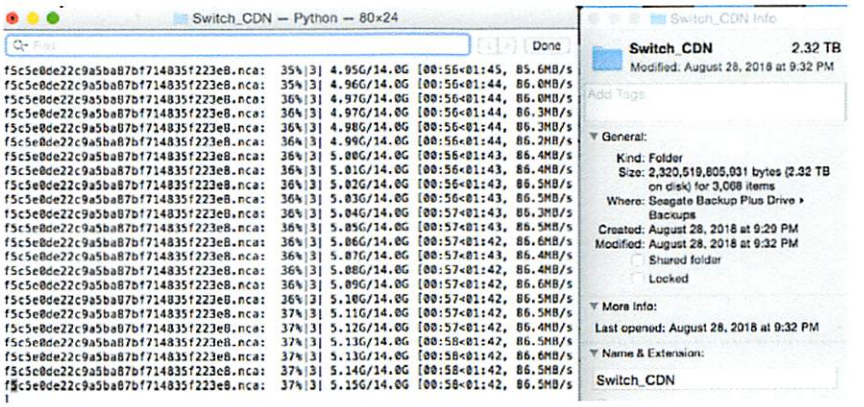
[7] "CDN" often refers to a Content Delivery Network which is a method by which data is transmitted by using a system of distributed servers that deliver the content based on your geographic location. This helps speed up data transfer.

[8] According to various online reference sites, "oml" typically means "Oh My Lord" in Internet slang.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



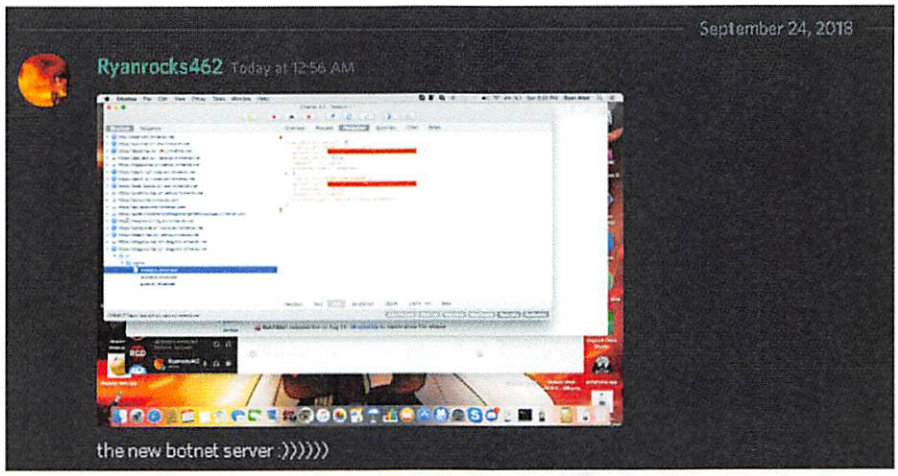
I also noticed that the "Switch_CDN" folder appears to have 2.32 TB of data, which is an extremely large amount of data. I also noticed that, according to the posted screenshots, the files appear to be backed up on a Seagate Backup Plus Drive:



b. On September 24, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted in the #general channel of his **SUBJECT DISCORD SERVER** an image showing what appears to be domains, along with the message: "the new botnet server :)))))))":[9]

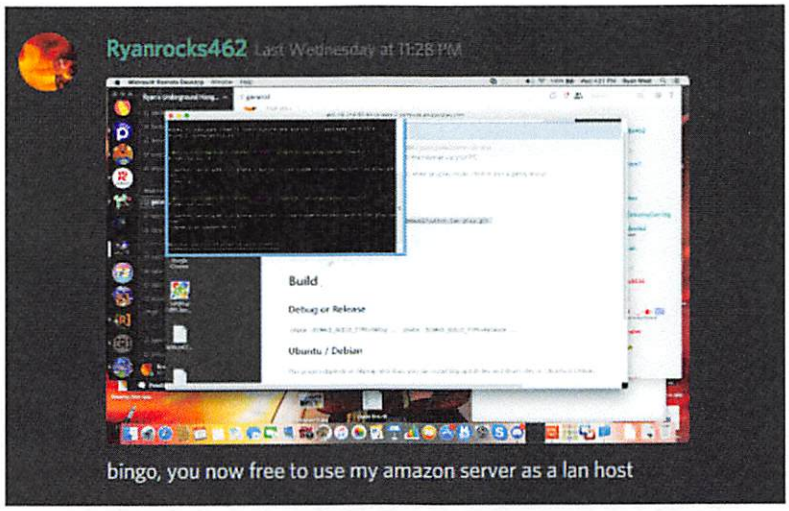
[9] A "botnet" typically refers to a network of compromised computers known as "bots" that are under the control of a cybercriminal or "bot herder." The bots are harnessed by the bot herder through the surreptitious installation of malware that provides the bot herder with remote access to, and control of, the compromised computers. A botnet may be used en masse, in a coordinated fashion, to deliver a variety of Internet-based attacks, including DDoS attacks, brute force password attacks, the transmission of spam emails, the transmission of phishing emails, and hosting communication networks for cybercriminals (e.g., acting as a proxy server for email communications).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



Based on my training and experience, I understand this message to indicate that HERNANDEZ is displaying external computers under his remote unauthorized control.

c. On October 17, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted a screenshot and stated that others were allowed to use his Amazon server as a LAN host:[10]

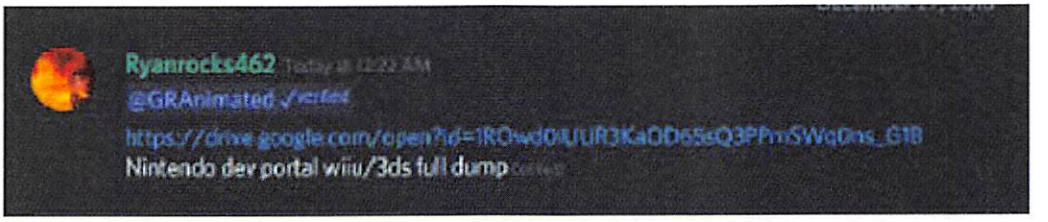


According to information provided by Nintendo, review of the image indicates Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** appears to be running a Switch play LAN host.

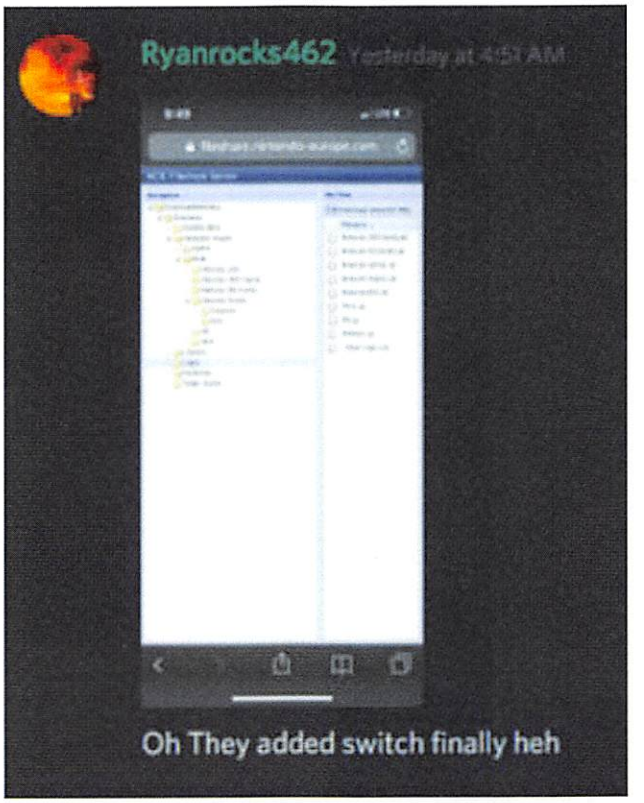
d. On December 12, 2018, Discord user ryanrocks462 **(SUBJECT**

[10] "LAN" typically refers to Local Area Network which refers to a group of interconnected computers.

ACCOUNT 3) (HERNANDEZ) posted a link to Google Drive that he claimed contained the Nintendo Developer Portal for Wii U and 3DS:[11]



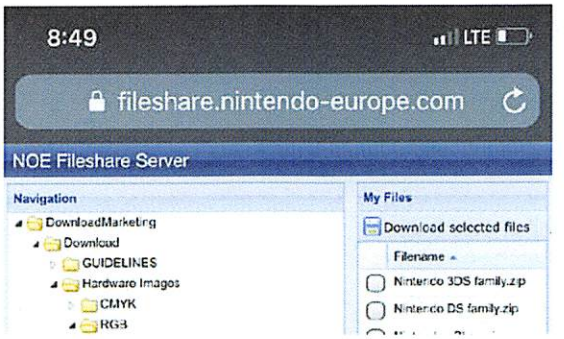
e. On December 16, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted an image of the file directory on fileshare.nintendo-europe.com and commented that the Switch had been added. The image appears to have been taken via a cellphone.



****

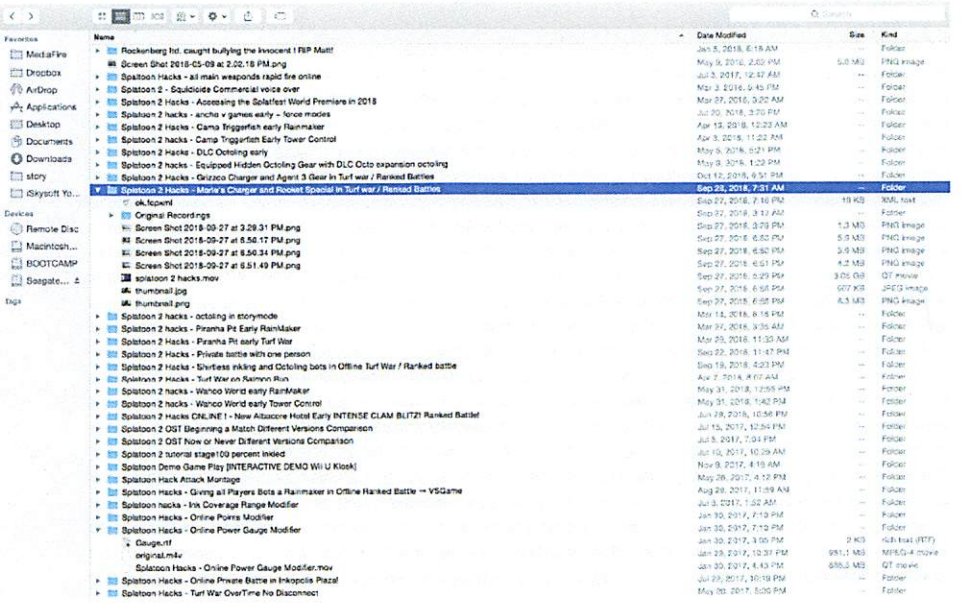
[11] According to information provided by Nintendo, the owner of the Google Drive folder was listed as Mary Landry (mary.landry@my.tccd.edu).

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970



This post suggests that HERNANDEZ may have access to a Nintendo file directory, related to the Nintendo 3DS and Switch consoles, among other things.

f. On January 20, 2019, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) posted a screenshot of a file directory, which appears to relate to Splatoon 2, a Nintendo product, along with the message: "lg [large] I should get to work uwu"[12]:



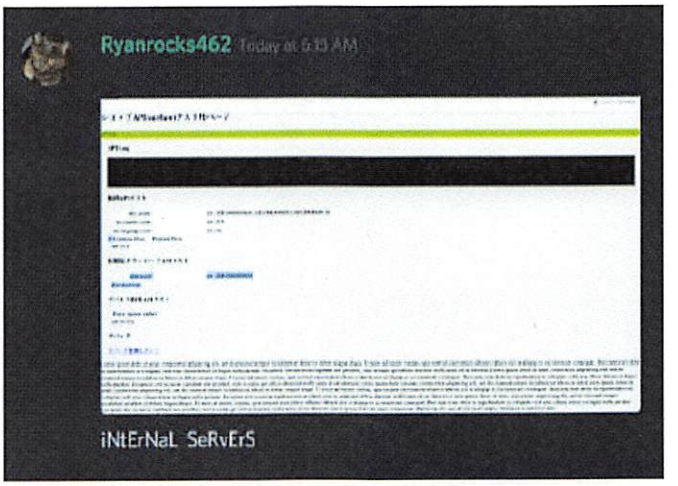
I also further noted that a Seagate drive (presumably, an external backup drive) was listed among the connected "Devices," which is consistent with the August 28 and September 3, 2018, Discord posts discussed above.

d. On February 4, 2019, Discord user ryanrocks462 **(SUBJECT**

[12] According to various online reference sites, "uwu" is Internet slang.

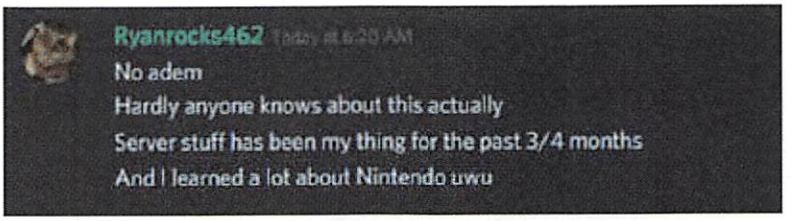
UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ACCOUNT 3) (HERNANDEZ) indicated that he needed to test a new piracy patch and posted multiple screenshots that he described as Nintendo internal servers, such as:



He further indicated that these images included Nintendo's internal eShop API testing server (which, as discussed above, is one of the server groups identified by Nintendo as having been compromised by HERNANDEZ):

User ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) further indicated that he had been working on Nintendo "Server stuff" for the past 3 to 4 months and had learned a lot about Nintendo:

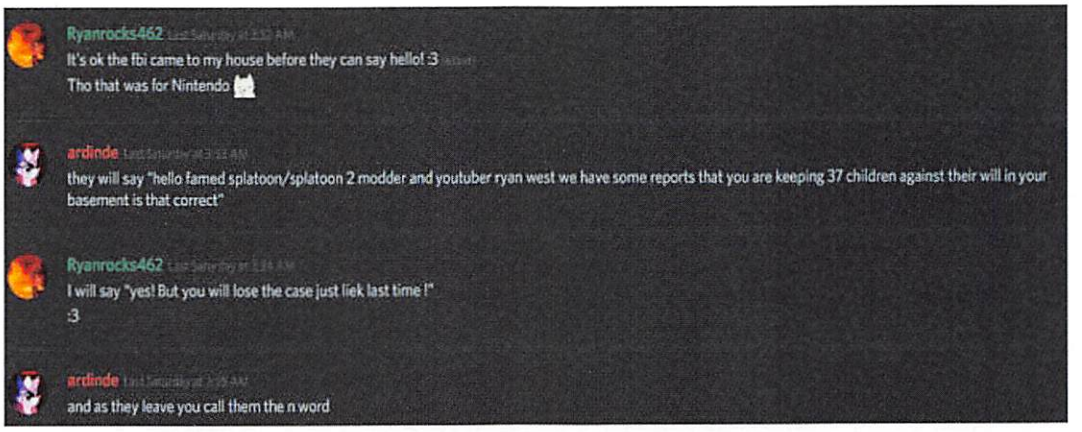


32. Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) also referenced his prior 2016 hack of Nintendo. For instance, on December 22, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) engaged in communications with other users in which they discussed HERNANDEZ's prior hack of Nintendo's Developer Portal. Initially, ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ)

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

asked others for available storage, either on their computer or on a Google Drive, indicating he need "like 400GB" for a backup that possibly included "30,000 + links" and "pre-release stuff to". User ryanrocks462 (HERNANDEZ) further suggested that the files related to "3ds/wiiu probably". User ryanrocks462 (HERNANDEZ) then told another user "U have to phish SDSG[,] Like anon did for me with the 16.7 sdk" and further explaining the phishing methodology. As set forth in the tweet by user **@ryanrocks462 (SUBJECT ACCOUNT 1)** (HERNANDEZ), above, HERNANDEZ thanked "anon" for helping with the leak of Switch SDK in October 2016. Based on my training and experience, and my involvement in this and the prior investigation, I believe that HERNANDEZ's comments relate to his prior hack of Nintendo's Developer Portal, discussed above.

33. Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) also referenced his prior contact with FBI agents. Specifically, on November 24, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) commented about how the FBI had previous come to his residence regarding Nintendo:



HERNANDEZ stated (likely humorously) that, if the FBI visited again, he would tell the FBI "you will lose the case just [like] last time !" I believe this is a reference to the fact that HERNANDEZ was not arrested or charged in relation to his prior Nintendo hack.

Twitter SUBJECT ACCOUNTS

34. Nintendo also provided the FBI with screenshots and summaries of various messages (or, "tweets") from two accounts believed to be used by RYAN HERNANDEZ,

namely, **User ID: 178776029, also known as username "@ryanrocks462" (SUBJECT ACCOUNT 1)** and **User ID: 715225783, also known as username "@ryanrocks562" (SUBJECT ACCOUNT 2)**. The FBI, through its investigation, confirmed that HERNANDEZ is the user of **SUBJECT ACCOUNT 1** and **SUBJECT ACCOUNT 2**.

35. According to records obtained from Twitter, account **@ryanrocks462 (SUBJECT ACCOUNT 1)** was created in 2010, and is associated with email address ryanrocks462@yahoo.com (SUBJECT ACCOUNT 4):

```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA512

account_id: 178776029
created_at: 2010-08-15 17:23:46 +0000
updated_at: 2018-09-13 20:01:18 +0000
email: ryanrocks462@yahoo.com
created_via: web
screen_name: ryanrocks462
time_zone: Pacific Time (US & Canada)
**********
```

Moreover, Twitter user **@ryanrocks462 (SUBJECT ACCOUNT 1)** was repeatedly accessed through the HERNANDEZ's home IP address (172.248.227.193) through at least October 26, 2018.[13] For instance,

```
account_id: 178776029
created_at: 2018-10-26 23:29:48 +0000
last_login_ip: 172.248.227.193
**********
```

36. Investigators have requested, but not yet received, subscriber records from Twitter pertaining to Twitter account **@ryanrocks562 (SUBJECT ACCOUNT 2)**. That said, as discussed herein, HERNANDEZ, the user of **SUBJECT ACCOUNT 1**, is also the user of **SUBJECT ACCOUNT 2**.

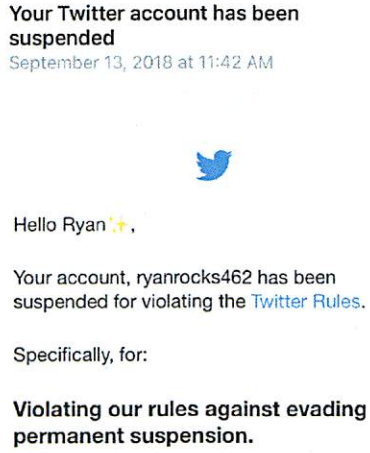
37. In September 2018, Twitter suspended **@ryanrocks462 (SUBJECT ACCOUNT 1)**. HERNANDEZ, using his other Twitter account **@ryanrocks562**

[13] Investigators only have Twitter IP log information for **SUBJECT ACCOUNT 1** through about November 19, 2018, the date records were received from Twitter. This predates the change in Internet service providers to AT&T and the new IP address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(SUBJECT ACCOUNT 2), complained about the suspension of **@ryanrocks462 (SUBJECT ACCOUNT 1)**, and otherwise made clear that he is the user of both accounts:

38. Similarly, on September 17, 2018, Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** posted about Twitter account **@ryanrocks462 (SUBJECT ACCOUNT 1)** having been suspended but that he was appealing, sharing the below image:



39. HERNANDEZ has referenced hacking activities on **@ryanrocks462 (SUBJECT ACCOUNT 1)**, such as:

a. As discussed above, in July 2017, Twitter user **@ryanrocks462 (SUBJECT ACCOUNT 1)** appeared to take credit for the 2016 hack of Nintendo's Developer Portal.

b. On September 29, 2017, Twitter user **@ryanrocks462 (SUBJECT**

ACCOUNT 1) tweeted about whether he should steal the Super Mario Odyssey demo unit "like I did with the 3ds carts before?" I believe this is a reference to HERNANDEZ's prior theft of Nintendo 3DS data.

c. On October 27, 2017, Twitter user **@ryanrocks462 (SUBJECT ACCOUNT 1)** tweeted that he was quitting the hacking scene, specifically: "I Officially quit any 'haxing' scene. They no longer interest me. I may have not done much, but I managed to what I could. :P –Ryan^^". On October 30, 2018, Twitter user **@ryanrocks462 (SUBJECT ACCOUNT 1)** sent another tweet: "Honestly, I'm moving on from computer shit now. It was fun, but now a days it's just boring to me. Maybe I'll be a pilot that seems fun hehe". Shortly thereafter, Twitter user **@ryanrocks462 (SUBJECT ACCOUNT 1)** followed up with a message: "I would like to announce due to some unexpected circumstances this account may 'possibly' be terminated by me soon."

d. Notably, FBI agents (including myself) contacted and interviewed HERNANDEZ at his Palmdale, California residence (TARGET RESIDENCE) regarding the 2016 hack of Nintendo on October 25, 2017 --- i.e., just days before these tweets. Accordingly, I believe that these messages are a direct reaction to law enforcement contact and interpret his statements as an acknowledgement by HERNANDEZ of his prior hacking ("haxing") activity. I also suspect that the realization of the FBI's awareness of and interest in his illegal conduct is the "unexpected circumstances" that prompted HERNANDEZ to contemplate deleting **SUBJECT ACCOUNT 1**.

e. HERNANDEZ did not ultimately delete or deactivate **SUBJECT ACCOUNT 1**. Rather, on November 7, 2017, Twitter user **@ryanrocks462 (SUBJECT ACCOUNT 1)** asked another Twitter user (@Govanify) for a recommendation for SSD encrypters and destroyers. This message suggests that HERNANDEZ was intending and/or attempting to encrypt and/or destroy stored data. Again, based on the timing, I suspect this relates to the 2016 hack of Nintendo and the recent law enforcement contact.

40. Twitter user **@ryanrocks562 (SUBJECT ACCOUNT 2)** (HERNANDEZ) likewise has referenced hacking and made statements pertinent to the investigation. For

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

instance,

a. On September 29, 2018, Twitter user **@ryanrocks562 (SUBJECT ACCOUNT 2)** (HERNANDEZ) tweeted an expression of appreciation for having found a "hacking community":

I further note that the avatar for **@ryanrocks562 (SUBJECT ACCOUNT 2)** appears to be the Link character from Nintendo's The Legend of Zelda franchise.

b. Also on September 29, 2018, Twitter user **@ryanrocks562 (SUBJECT ACCOUNT 2)** (HERNANDEZ) tweeted an image of the Spongebob Squarepants cartoon character wearing an FBI hat, with the message: "Hi @NintendoAmerica":

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Notably, this tweet came only days after Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) mockingly discussed the prior contact by FBI agents regarding Nintendo, discussed above.

c. On December 9, 2018, Twitter user **@ryanrocks562 (SUBJECT ACCOUNT 2)** (HERNANDEZ) announced that another Twitter user (@Cylints) had compromised his Epic games account and asked that user whether he/she used a "classic Phishing attack, or gather from another site database leak."

Apple TARGET ACCOUNT

41. Based on my training and experience, I recognize Apple devices, both a laptop and iPhone, and Apple (Mac) user interface in various images posted by HERNANDEZ in the accounts discussed above. I also know that Apple devices typically are associated with Apple iCloud accounts. I further know that iCloud accounts are used, among other things, to back-up data from user's associated Apple devices, and, under default settings, such activity is regularly done automatically.

42. The records and information provided by Nintendo included tweets by the user of **@ryanrocks562 (SUBJECT ACCOUNT 2)** and **@ryanrocks462 (SUBJECT ACCOUNT 1)**, which I know to be accessible on a variety of phones, tablets, as well as computers. This material also included posts by Discord user ryanrocks462 **(SUBJECT ACCOUNT 3)** (HERNANDEZ) that included screenshots and photographs that appear to have originated from a phone.

43. According to records obtained from Apple, it appears that RYAN HERNANDEZ has purchased numerous iPhones since 2013, including an iPhone 7 in 2016 and an iPhone X in November 2017:

purchase date	product description	customer name	contact name	dsid	apple logon id
2009-04-06 00:00:00	IPOD TOUCH (2ND GEN) 8GB-USA	ryan hernandez		1092155705	ryanrocks462@yahoo.com
2013-03-10 00:00:00	SVC,IPHONE 5,GSM,16GB,BLACK,CI	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2013-03-10 00:00:00	IPHONE 5 BLACK 16GB AT&T-USA	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2013-03-10 00:00:00	SVC,IPHONE 5,GSM,16GB,BLACK,CI	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2013-03-26 00:00:00	IPOD SHUFFLE 2GB SILVER-USA	ryan hernandez	ryan hernandez	1092155705	ryanrocks462@yahoo.com
2013-10-25 00:00:00	IPHONE 5S GOLD 32GB-USA	Ruben Hernandez	Ruben Hernandez	1710515926	ryanrocks463@yahoo.com
2014-07-05 00:00:00	MBP 15.4/2.3GHZ/16GB/512GB FL	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2014-11-12 00:00:00	IPHONE 6 GOLD 64GB AT&T-USA	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2014-12-30 00:00:00	IPHONE 6 SPACE GRAY 64GB AT&T-	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2015-09-30 00:00:00	IPHONE 6S GOLD 128GB AT&T-USA	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2016-09-12 00:00:00	IPHONE 7 JET BLACK 256GB AT&T-L	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2016-09-13 00:00:00	SVC,IPHONE 7,GSM,256GB,JBLK,CI/	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com
2017-11-21 00:00:00	IPHONE X SPACE GRAY 256GB AT&'	Ruben Hernandez		1710515926	ryanrocks463@yahoo.com

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Each phone is listed in the name of HERNANDEZ's father and associated with one of HERNANDEZ's Yahoo emails addresses, namely, ryanrocks463@yahoo.com (SUBJECT ACCOUNT 6), and the TARGET RESIDENCE.

44. From records obtained from Apple, investigators identified three Apple iCloud accounts associated with HERNANDEZ; but, according to activity logs, only one, **Apple ID 1710515926**, associated with **ryanrocks462@icloud.com (SUBJECT ACCOUNT 7)**, is in use.[14] **SUBJECT ACCOUNT 7** is associated with ryanrocks463@yahoo.com (SUBJECT ACCOUNT 6) and is registered in the name of Ruben Hernandez (HERNANDEZ's father) of Palmdale, California:

Apple ID	DS ID	Account Typ	Login Alias	First Nam	Last Nam	Country	Languag
ryanrocks463@yahoo.com	1710515926	Full iCloud	ryanrocks462@icloud.com	Ruben	Hernandez	United States	US-EN

The account is linked to iTunes and Gamecenter activity exclusively in the name of RYAN HERNANDEZ of the Palmdale, California TARGET RESIDENCE.

45. The iCloud logs obtained from Apple for **Apple ID 1710515926 (SUBJECT ACCOUNT 7)** suggest significant, almost daily, account activity during the entire period for which records were provided, from November 22, 2018 to December 11, 2018. Further, the vast majority of the log activity for **SUBJECT ACCOUNT 7** is associated with HERNANDEZ's TARGET RESIDENCE IP addresses (172.248.227.193, until November 27, 2018, and 76.232.194.142, thereafter). A sample excerpt from a portion of the activity on December 4, 2018 is below:

1710515926	Service=ICLOUDDRIVE	timestamp="Tue Dec 04 17:41:22.103 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=ICLOUDDRIVE	timestamp="Tue Dec 04 17:41:22.100 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:21.793 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:21.786 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=ICLOUDDRIVE	timestamp="Tue Dec 04 17:41:21.358 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=ICLOUDDRIVE	timestamp="Tue Dec 04 17:41:21.353 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:20.355 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=CONTACTS	timestamp="Tue Dec 04 17:41:19.101 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:18.964 PST 2018"	Device Type and OS="MacBookPro11,3" "OSX;10.10.x"	76.232.194.142
1710515926	Service=SAFARIBROWSINGHISTORY	timestamp="Tue Dec 04 17:41:18.962 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=CONTACTS	timestamp="Tue Dec 04 17:41:18.776 PST 2018"	Device Type and OS=	76.232.194.142
1710515926	Service=CONTACTS	timestamp="Tue Dec 04 17:41:18.651 PST 2018"	Device Type and OS=	76.232.194.142

Based on my review of evidence, I know that HERNANDEZ maintained an active iCloud account **(SUBJECT ACCOUNT 7)** at the same time he was engaged in the threat activity

[14] The other two iCloud accounts (Apple ID 1092155705 and 1706835673) are associated with emails ryanrocks462@yahoo.com (SUBJECT ACCOUNT 4) and ryanrocks562@yahoo.com (SUBJECT ACCOUNT 5), respectively, and in the name RYAN HERNANDEZ.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

under investigation.

Google TARGET ACCOUNT

46. From various screenshots posted by RYAN HERNANDEZ, it appears that HERNANDEZ uses Google Chrome. I further know that HERNANDEZ utilizes a wide variety of Google services. For instance, according to records obtained from Google, his Google account **(Account ID 279578011651)**, associated with email **ryanrocks562@gmail.com (SUBJECT ACCOUNT 8)** is associated with numerous Google products and services, including email, Google Chrome, Google Drive and YouTube, as set forth in the subscriber information below:

```
GOOGLE SUBSCRIBER INFORMATION
Name: Ryan West
e-Mail: ryanrocks562@gmail.com
Services: Android, Blogger, Chromeos Login, Glass, Gmail, Google
AdSense, Google AdWords, Google Calendar, Google Chrome Sync,
Google Docs, Google Drive, Google Hangouts, Google Maps Engine,
Google My Maps, Google Payments, Google Photos, Google Play,
Google Play Music, Google Sites, Google URL Shortener, Google
Voice, Google+, Has Google Profile, Has Madison Account, Has
Plusone, Location History, Web & App Activity, YouTube, YouTube
CMS, iGoogle
Recovery e-Mail: ryanrocks462@yahoo.com
Created on: 2010/08/04-22:33:32-UTC
Terms of Service IP: 98.148.168.104, on 2010/08/04-22:33:32-UTC
SMS: +16613613779 [US]
Alternate e-Mail(s): ryanrocks462@yahoo.com
Google Account ID: 279578011651
Last Logins: 2018/11/30-06:32:22-UTC, 2018/11/12-20:13:57-UTC,
2018/11/11-23:34:44-UTC
```

The recovery and alternate email addresses are both ryanrocks462@yahoo.com (SUBJECT ACCOUNT 4), and the associated phone number is the same as HERNANDEZ's Yahoo (Oath) accounts.

47. According to Google IP logs, which were provided on about December 19, 2018, **ryanrocks562@gmail.com (SUBJECT ACCOUNT 8)** was accessed through HERNANDEZ's home IP addresses (172.248.227.193 and 76.232.194.142) at the time HERNANDEZ is believed to have been engaging in the illegal activity discussed herein:

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Time	IP Address	Type
2018/11/30-06:32:22-UTC	76.232.194.142	Login
2018/11/12-20:17:36-UTC	2606:6000:50cc:8000:195:6977:74e5:8fd2	Logout
2018/11/12-20:13:57-UTC	2606:6000:50cc:8000:195:6977:74e5:8fd2	Login
2018/11/11-23:34:44-UTC	2606:6000:50cc:8000:1c13:77e4:2563:e1de	Login
2018/10/21-20:37:55-UTC	172.248.227.193	Login
2018/07/14-10:59:57-UTC	172.248.227.193	Login

Moreover, I know that users of online accounts such as Google may, in fact often, remain logged into accounts for extended periods of time. Here, the last action logged indicates a login on November 30, 2018, from HERNANDEZ's home IP address at the TARGET RESIDENCE, without a logout through the date of records production. I also note that this time period corresponds with when HERNANDEZ is suspect of engaging in criminal activity over the Internet.

48. Based on my training and experience, I know that Google logs and retains a substantial amount of information about its customers. Unless specific steps are taken to change default settings or to conceal or delete records of activity, this information should include, among many other things, customers' Internet activity, including their web browsing and search history, while logged into a Google account or through a Google product, such as Chrome. I also know that the type of crime at issue here necessitates use of the Internet and electronic devices. As discussed herein, HERNANDEZ was very active on various online accounts, including the **TARGET ACCOUNTS**. Accordingly, based on these IP records and HERNANDEZ's general use of Google Chrome and other Google accounts, there is probable cause to believe that Google possesses information that is evidence of criminal conduct.

49. Accordingly, I am also seeking *limited* authorization to search the web browsing and search activity and non-content account records and information, as described in Attachment B-4, associated with HERNANDEZ's Google account, **ryanrocks562@gmail.com (SUBJECT ACCOUNT 8)**. I am not seeking authorization to search content of the email account itself.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

BACKGROUND REGARDING TWITTER

50. Twitter owns and operates a free-access social-networking website of the same name that can be accessed at http://www.twitter.com. Twitter allows its users to create their own profile pages, which can include a short biography, a photo of themselves, and location information. Twitter also permits users to create and read character-limited messages called "Tweets," and to restrict their "Tweets" to individuals whom they approve. These features are described in more detail below.

51. Upon creating a Twitter account, a Twitter user must create a unique Twitter username and an account password, and the user may also select a different name of 20 characters or fewer to identify his or her Twitter account. The Twitter user may also change this username, password, and name without having to open a new Twitter account.

52. Twitter asks users to provide basic identity and contact information, either during the registration process or thereafter. This information may include the user's full name, e-mail addresses, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers. For each user, Twitter may retain information about the date and time at which the user's profile was created, the date and time at which the account was created, and the Internet Protocol ("IP") address at the time of sign-up. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access a given Twitter account.

53. A Twitter user can post a personal photograph or image (also known as an "avatar") to his or her profile, and can also change the profile background or theme for his or her account page. In addition, Twitter users can post "bios" to their profile pages.

54. Twitter also keeps IP logs for each user. These logs contain information about the user's logins to Twitter including, for each access, the IP address assigned to the user and the date stamp at the time the user accessed his or her profile.

55. As discussed above, Twitter users can use their Twitter accounts to post "Tweets" of 280 (formerly, 140) characters or fewer. Each Tweet includes a timestamp that

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

displays when the Tweet was posted to Twitter. Twitter users can also "favorite," "retweet," or reply to the Tweets of other users. In addition, when a Tweet includes a Twitter username, often preceded by the @ sign, Twitter designates that Tweet a "mention" of the identified user. In the "Connect" tab for each account, Twitter provides the user with a list of other users who have "favorited" or "retweeted" the user's own Tweets, as well as a list of all Tweets that include the user's username (i.e., a list of all "mentions" and "replies" for that username).

56. Twitter users can include photographs or images in their Tweets. Each Twitter account also is provided a user gallery that includes images that the user has shared on Twitter, including images uploaded by other services.

57. Twitter users can also opt to include location data in their Tweets, which will reveal the users' locations at the time they post each Tweet. This "Tweet With Location" function is off by default, so Twitter users must opt in to the service. In addition, Twitter users may delete their past location data.

58. When Twitter users want to post a Tweet that includes a link to a website, they can use Twitter's link service, which converts the longer website link into a shortened link that begins with http://t.co. This link service measures how many times a link has been clicked.

59. A Twitter user can "follow" other Twitter users, which means subscribing to those users' Tweets and site updates. Each user profile page includes a list of the people who are following that user (i.e., the user's "followers" list) and a list of people whom that user follows (i.e., the user's "following" list). Twitter users can "unfollow" users whom they previously followed, and they can also adjust the privacy settings for their profile so that their Tweets are visible only to the people whom they approve, rather than to the public (which is the default setting). A Twitter user can also group other Twitter users into "lists" that display on the right side of the user's home page on Twitter. Twitter also provides users with a list of "Who to Follow," which includes a few recommendations of Twitter accounts

that the user may find interesting, based on the types of accounts that the user is already following and who those people follow.

60. In addition to posting Tweets, a Twitter user can also send Direct Messages (DMs) to one of his or her followers. These messages are typically visible only to the sender and the recipient, and both the sender and the recipient have the power to delete the message from the inboxes of both users. As of January 2012, Twitter displayed only the last 100 DMs for a particular user, but older DMs are stored on Twitter's database.

61. Twitter users can configure the settings for their Twitter accounts in numerous ways. For example, a Twitter user can configure his or her Twitter account to send updates to the user's mobile phone, and the user can also set up a "sleep time" during which Twitter updates will not be sent to the user's phone.

62. Twitter includes a search function that enables its users to search all public Tweets for keywords, usernames, or subject, among other things. A Twitter user may save up to 25 past searches.

63. Twitter users can connect their Twitter accounts to third-party websites and applications, which may grant these websites and applications access to the users' public Twitter profiles.

64. If a Twitter user does not want to interact with another user on Twitter, the first user can "block" the second user from following his or her account.

65. In some cases, Twitter users may communicate directly with Twitter about issues relating to their account, such as technical problems or complaints. Social-networking providers like Twitter typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. Twitter may also suspend a particular user for breaching Twitter's terms of service, during which time the Twitter user will be prevented from using Twitter's services.

66. As explained herein, information stored in connection with a Twitter account may provide crucial evidence of the "who, what, why, when, where, and how" of the

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, a Twitter user's account information, IP log, stored electronic communications, and other data retained by Twitter, can indicate who has used or controlled the Twitter account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, profile contact information, communications, "tweets" (status updates) and "tweeted" photos (and the data associated with the foregoing, such as date and time) may be evidence of who used or controlled the Twitter account at a relevant time. Further, Twitter account activity can show how and when the account was accessed or used. For example, as described herein, Twitter logs the Internet Protocol (IP) addresses from which users access their accounts along with the time and date. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the account access and use relating to the crime under investigation. Such information allows investigators to understand the geographic and chronological context of Twitter access, use, and events relating to the crime under investigation. Additionally, Twitter builds geo-location into some of its services. If enabled by the user, physical location is automatically added to "tweeted" communications. This geographic and timeline information may tend to either inculpate or exculpate the Twitter account owner. Last, Twitter account activity may provide relevant insight into the Twitter account owner's state of mind as it relates to the offense under investigation. For example, information on the Twitter account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a criminal plan) or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

67. Therefore, the computers of Twitter are likely to contain the material described above, including stored electronic communications and information concerning subscribers and their use of Twitter, such as account access information, transaction information, and other account information.

BACKGROUND REGARDING DISCORD

68. Discord owns and operates a free-access, all-in-one voice and text chat application and website of the same name that can be accessed at http://www.discordapp.com. Discord is a "cross-platform" application, which is available for Microsoft Windows, Mac OS, Android, Apple iOS, and Linux operating systems. As of December 2018, Discord claimed approximately 200 million users, and targets gamers and the gaming community.

69. Discord allows its users to establish accounts, which they can then use to communicate with other Discord users. Discord also allows users to create servers, or chat rooms, to host discussions on any topic. A server can be configured as public, meaning anyone can join, or it can be configured to be private. To participate in a private server, a user must be invited by another user who already belongs to that private server. Invitations can be configured to expire after a short period of time, limited to the number of times an invitation can be shared, and even be configured to limit a user to participating in the group one time.

70. Within a specific server, Discord provides text chat capabilities, to include the ability to upload and share images. Discord also provides voice chat capabilities in which users are able to directly call one or more users at a time, allowing for group voice chats, similar to other voice service providers such as Skype and TeamSpeak.

71. Similar to other communication platforms, Discord users are able to create and maintain a friends list, participate in multiple servers or communication channels, and set their current status indicator to appear online, away, or invisible to other users.

72. When signing up for a Discord account, the user must agree to Discord's Terms of Service.[15] Discord's terms of service, Rules of Conduct and Usage state, "You agree not to use the Service in order to: violate any applicable laws or regulations, or promote or encourage any illegal activity…"

[15] Discord's Terms of Service may be accessed online: https://discordapp.com/tos.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

73. Discord asks users to provide basic contact information to Discord, either during the registration process or thereafter. The information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code) telephone numbers, screen names, websites, and other personal identifiers. Discord also assigns a user identification number to each account.

74. Discord may also retain Internet Protocol ("IP") logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Discord, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Discord profile, that user's IP log would reflect the fact the user viewed the profile, and would show when and from what IP address the user did so.

75. Social networking providers like Discord typically retain additional information about their users' accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Discord users may communicate directly with Discord about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Discord typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications.

76. The computers or servers of Discord are likely to contain the material just described, including stored electronic communications and information concerning subscribers and their use of Discord, such as account access information, transaction information, and account activation.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

BACKGROUND REGARDING APPLE AND ICLOUD

77. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

78. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage.

79. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

80. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

81. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

82. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs enables iCloud to be used to synchronize webpages opened in the Safari web browsers on all of the user's Apple devices. iWorks Apps, a suite of productivity apps (Pages, Numbers, and Keynote), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords,

credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

83. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

84. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices.

85. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

86. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

87. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

88. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

89. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

90. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

91. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that

computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

92. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWorks and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

93. In this case, I am investigating hacking of a victim network and the download of nonpublic data and information, which necessitates the use of electronic devices and the Internet. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

94. The kinds of records maintained by Apple may help identify additional fraudulent and illegal conduct, identify suspects (who often use false names, aliases, and online monikers), and determine how stolen data was obtained, transferred, stored, and possibly distributed. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

95. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

96. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

97. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, emails, instant messages, Internet activity, documents,

and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

98. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

BACKGROUND REGARDING GOOGLE SERVICES

99. In my training and experience, I have learned that Google provides a wide variety of on-line services, including electronic mail ("e-mail") access and instant messaging (otherwise known as "chat" messaging), to the general public. Google provides subscribers e-mail and chat accounts at the domain name "@gmail.com." Google also allows subscribers to register a custom domain name and set up Google services such as chat and e-mail using that domain name instead of "@gmail.com." Google also hosts domains and provides a multitude of services that can be linked and managed through a common account.

A. Subscriber Records and Account Content

100. Subscribers obtain an account by registering with Google. When doing so, e-mail providers like Google ask the subscriber to provide certain personal identifying information. This information can include the subscriber's full name, physical address, telephone numbers and other identifiers, alternative e-mail addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users, and to help establish who has dominion and control over the account.

101. E-mail providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (i.e., session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging

into the account via Google's websites), and other log files that reflect usage of the account. In addition, e-mail providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the e-mail account.

102. In some cases, e-mail account users will communicate directly with an e-mail service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. E-mail providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation, because the information can be used to identify the account's user or users.

103. In general, an e-mail that is sent to a Google subscriber is stored in the subscriber's "mail box" on Google's servers until the subscriber deletes the e-mail. When the subscriber sends an e-mail, it is initiated at the user's computer, transferred via the Internet to Google servers, and then transmitted to its end destination. Google often maintains a copy of received and sent e-mails. Unless the sender specifically deletes an e-mail from the Google server, the e-mail can remain on the system indefinitely. Even if the subscriber deletes the e-mail, it may continue to be available on Google's servers for some period of time.

104. A sent or received e-mail typically includes the content of the message, source and destination addresses, the date and time at which the e-mail was sent, and the size and length of the e-mail. If an e-mail user writes a draft message but does not send it, that message may also be saved by Google but may not include all of these categories of data.

105. In addition to e-mail and chat, Google offers subscribers numerous other services including: Android, Blogger, Google Alerts, Google Calendar, Google Chrome

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Sync, Google Cloud Print, G-Suite, Google Developers Console, Google Drive, Google Hangouts, Google Maps, Google Payments, Google Photos, Google Search Console, Google Voice, Google+, Google Profile, Location History, Web & Activity, and YouTube, among others. Thus, a subscriber to a Google account can also store files, including address books, contact lists, calendar data, photographs and other files, on servers maintained and/or owned by Google. For example, Google Calendar is a calendar service that users may utilize to organize their schedule and share events with others. Google Drive may be used to store data and documents, including spreadsheets, written documents (such as Word or Word Perfect) and other documents that could be used to manage a website. Google Photos can be used to create photo albums, store photographs, and share photographs with others and "You Tube," allows users to view, store and share videos. Google Search Console records a Google account user's search queries. And Google Web & Activity records certain browsing history depending on whether the account holder is logged into their account. Like many internet service companies, the services Google offers are constantly changing and evolving.

106. Google also offers a suite of cloud computing services that runs on the same infrastructure that Google uses internally for its end-user products, such as Google Search and YouTube. Alongside a set of management tools, it provides a series of modular cloud services including computing, data storage, data analytics and machine learning to customers.

107. Based upon my training and experience, all of these types of information may be evidence of crimes under investigation. Stored e-mails and chats not only may contain communications relating to crimes, but also help identify the participants in those crimes. For example, address books and contact lists may help identify and locate co-conspirators. Similarly, photographs and videos of co-conspirators may help identify their true identities, as opposed to supposed identities that they have used in telephone or e-mail communications. Documents (such as Google sheets used to communicate with victim computers), may identify the scope of the criminal activity. And calendar data may reveal the timing and extent of criminal activity. Search and browsing history can also be extremely

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

useful in identifying those using anonymous online accounts and may also constitute direct evidence of the crimes under investigation to the extent the browsing history or search history might include searches and browsing history related to computer intrusions, victims, trafficking in stolen data and other evidence of the crimes under investigation or indications of the true identity of the account users.

108. Google is also able to provide information that will assist law enforcement in identifying other accounts associated with the **SUBJECT ACCOUNT(S)**, namely, information identifying and relating to other accounts used by the same subscriber. This information includes any forwarding or fetching accounts[16] relating to the **SUBJECT ACCOUNT(S)**, all other Google accounts linked to the **SUBJECT ACCOUNT(S)** because they were accessed from the same computer (referred to as "cookie overlap"), all other Google accounts that list the same SMS phone number as the **SUBJECT ACCOUNT(S)**, all other Google accounts that list the same recovery e-mail address[17] as do the **SUBJECT ACCOUNT(S)**, and all other Google accounts that share the same creation IP address as the **SUBJECT ACCOUNT(S)**. Information associated with these associated accounts will assist law enforcement in determining who controls the **SUBJECT ACCOUNT(S)** and will also help to identify other e-mail accounts and individuals relevant to the investigation.

B. Google Location History and Location Reporting

109. According to Google's website, "Location Reporting" allows Google to periodically store and use a device's most recent location data in connection with the Google Account connected to the device. "Location History" allows Google to store a history of location data from all devices where a user is logged into their Google Account and have enabled Location Reporting. According to Google "when you turn on Location Reporting

---

[16] A forwarding or fetching account related to the **SUBJECT ACCOUNT(S)** would be a separate e-mail account that can be setup by the user to receive copies of all of the e-mail sent to the **SUBJECT ACCOUNT(S)**.

[17] The recovery e-mail address is an additional e-mail address supplied by the user that is used by Google to confirm your username after you create an e-mail account, help you if you are having trouble signing into your Google account or have forgotten your password, or alert you to any unusual activity involving user's Google e-mail address.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

for a device like your iPhone or iPad, it lets Google periodically store and use that device's most recent location data in connection with your Google Account." How often Location Reporting updates location data is not fixed. Frequency is determined by factors such as how much battery life the device has, if the device is moving, or how fast the device is moving. Google's location services may use GPS, Wi-Fi hotspots, and cellular network towers to determine an account holder's location.

110. Based on the above, I know that if a user of the **SUBJECT ACCOUNT(S)** utilizes a mobile device to access the respective account identified in Attachment A and has not disabled location services on his or her device/s or through the Google account settings, Google may have detailed records of the locations at which the account holders utilized the mobile device/s. This type of evidence may further assist in identifying the account holders, and lead to the discovery of other evidence of the crimes under investigation.

111. I know that Google's Android service collects and stores identifying information about an Android smart phone used to access the Google account, including the International Mobile Equipment Identifier (IMEI), International Mobile Subscriber Identity (IMSI), telephone number and mobile carrier code. I know that Google's Location History service periodically queries the physical location of a device that is currently accessing a Google account through the device's GPS, nearby Wi-Fi network IDs and cellular tower information and records a history of device movements in Google's servers.

PRESERVATION REQUESTS

112. On the listed dates, the FBI sent preservation requests to the Providers requesting that they preserve all evidence related to the **TARGET ACCOUNTS**:

ACCOUNT	**DATE**
Twitter account **@ryanrocks462 (SUBJECT ACCOUNT 1)**	1/28/19
Twitter account **@ryanrocks562 (SUBJECT ACCOUNT 2)**	1/28/19
Discord account **ryanrocks462#8138 (SUBJECT ACCOUNT 3)**	1/28/19

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

Discord server "**Ryan's Underground Hangout**" (**SUBJECT DISCORD SERVER**)	1/28/19
Apple ID: 1710515926, associated with ryanrocks462@icloud.com (**SUBJECT ACCOUNT 7**)	None
Account ID: 279578011651, associated with ryanrocks562@gmail.com (**SUBJECT ACCOUNT 8**)	None

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

113. Pursuant to Title 18, United States Code, Section 2703(g), this application and affidavit for a search warrant seeks authorization to permit each Provider, and its agents and employees, to assist agents in the execution of this warrant. Once issued, the search warrant will be presented to the Provider with direction that it identify the account(s) described in the corresponding Attachment A to this affidavit, as well as other subscriber and log records associated with the account, as set forth in Section I of Attachment B to this affidavit.

114. The search warrant will direct the Provider to create an exact copy of the specified account and records, including an exact copy of the contents of the hard disk drive or drives installed on the server associated with the pertinent **SUBJECT ACCOUNT(S)**, or the original drives.

115. I, and/or other law enforcement personnel will thereafter review the copy of the electronically stored data, and identify from among that content those items that come within the items identified in Section II to Attachment B, for seizure.

116. Analyzing the data contained in the forensic image may require special technical skills, equipment, and software. It could also be very time-consuming. Searching by keywords, for example, can yield thousands of "hits," each of which must then be reviewed in context by the examiner to determine whether the data is within the scope of the warrant. Merely finding a relevant "hit" does not end the review process. Keywords used originally need to be modified continuously, based on interim results. Certain file formats, moreover, do not lend themselves to keyword searches, as keywords, search text, and many

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

common e-mail, database and spreadsheet applications do not store data as searchable text. The data may be saved, instead, in proprietary non-text format. And, as the volume of storage allotted by service providers increases, the time it takes to properly analyze recovered data increases, as well. Consistent with the foregoing, searching the recovered data for the information subject to seizure pursuant to this warrant may require a range of data analysis techniques and may take weeks or even months. All forensic analysis of the data will employ only those search protocols and methodologies reasonably designed to identify and seize the items identified in Section II of Attachment B to the warrant.

CONCLUSION

117. Based on the forgoing, I request that the Court issue the proposed search warrants. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that - has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i). Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. Accordingly, by this Affidavit and Warrant I seek authority for the government to search all of the items specified in Section I, Attachment B (attached hereto and incorporated by reference herein) to the Warrant, and specifically to seize all of the data, documents and records that are identified in Section II to that same Attachment.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

REQUEST FOR SEALING

118. I further request that the Court order that all papers in support of this application, including the affidavit and search warrants, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the target(s) of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Joel Martini, Affiant
Special Agent
Federal Bureau of Investigation

SUBSCRIBED and SWORN to before me this 21 day of February, 2019.

HONORABLE MARY ALICE THEILER
United States Magistrate Judge

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-1

Twitter Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following account(s):

i. **User ID: 178776029**, also known as "**@ryanrocks462**"

ii. **User ID: 715225783**, also known as "**@ryanrocks562**"

("**SUBJECT ACCOUNTS**") as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by Twitter, Inc., an e-mail provider headquartered at 1355 Market Street, Suite 900, San Francisco, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-1

Items to be Seized

I. Information to be disclosed by Twitter, for search:

To the extent that the information described in Attachment A-1 is within the possession, custody, or control of Twitter, Inc. ("Provider"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-1:

(a) All "Tweets" (message posts) and Direct Messages sent, received, "favorited," or retweeted by the account, including all photographs, video clips, or images included in those Tweets and Direct Messages, associated with the account from **July 1, 2016 to the present**;

(b) All identity and contact information, including full name, email address, physical address (including city, state, and zip code), date of birth, gender, hometown, occupation, and other personal identifiers;

(c) All past and current usernames, account passwords, and names associated with the account;

(d) The dates and times at which the account and profile were created, and the Internet Protocol ("IP") address at the time of sign-up;

(e) All IP logs and other documents showing the IP address, date, and time of each login to the account;

(f) All data and information associated with the profile page, including photographs, biographies ("bios"), and profile backgrounds and themes;

(g) [BLANK]

(h) All photographs and images in the user gallery for the account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(i) All location data associated with the account, including all information collected by the "Tweet With Location" service and information regarding locations where the account was accessed;

(j) All information about the account's use of Twitter's link service, including all longer website links that were shortened by the service, all resulting shortened links, and all information about the number of times that a link posted by the account was clicked;

(k) All data and information that has been deleted by the user;

(l) A list of all of the people that the user follows on Twitter (*i.e.*, the user's "following" list);

(m) A list of all users that the account has "unfollowed" or blocked;

(n) All "lists" created by the account, including friend or buddy lists;

(o) All information on the "Who to Follow" list for the account;

(p) All privacy and account settings;

(q) All records of Twitter searches performed by the account, including all past searches saved by the account;

(r) All information about connections between the account and third-party websites and applications;

(s) All records pertaining to communications between Twitter and any person regarding the user or the user's Twitter account, including contacts with support services, and all records of actions taken, including suspensions of the account.

The Provider is hereby ordered to disclose the above information to the government **within 14 days** of service of this warrant.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), those violations occurring since at least October 2016 to the present, including, for each account or identifier listed on Attachment A-1, information pertaining to the following matters:

(a) Evidence of any attempt or plan to engage in computer hacking activity; access to computers or servers of Nintendo or to files, information, or data related to Nintendo products; the possession, use, or transfer of Nintendo authentication credentials, stolen property, or files, information, or data related to Nintendo or Nintendo products; research or reconnaissance about Nintendo products, release dates, or developer tools;

(b) Evidence of prior contact with law enforcement, including the Federal Bureau of Investigation (FBI);

(c) Evidence of the account user's true name, identity and use of aliases or monikers;

(d) Evidence of the account user's ownership, use, or access to other online accounts, including, but not limited to, email, social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive) accounts;

(e) Evidence of efforts to encrypt data or destroy evidence;

(f) Evidence indicating the account user's state of mind as it relates to the crime under investigation;

(g) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

(h) Any address lists or buddy/contact lists associated with the specified account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(i) All messages, documents and profile information, attachments, or other data that otherwise constitute or identify the fruits or proceeds, or the instrumentalities, of the criminal violations of Title 18, United States Code, described above.

(j) All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

(k) Any and all other log records, including IP address captures, associated with the specified account;

(l) Any records of communications between Provider, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This includes, but is not limited to, records of contacts between the subscriber and Provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

(m) All messages, documents and profile information, attachments, or other data that that identify person(s) who communicated with the account user about matters relating to the offense conduct, as described in paragraph (a), above, including records that help reveal their whereabouts. This includes, but is not limited to, an individual referred to as "anon."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-2

Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following account(s):

i. **User ID: 451537312900317201**, also known as username "**ryanrocks462#8138**" ("**SUBJECT ACCOUNT**")

ii. **Server ID: 419619233622654986**, also known as "**Ryan's Underground Hangout**" ("**SUBJECT DISCORD SERVER**")

as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by Discord, Inc., an e-mail provider headquartered at 444 De Haro St., Suite 200, San Francisco, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-2

Items to be Seized

I. Information to be disclosed by Discord, for search:

To the extent that the information described in Attachment A-2 is within the possession, custody, or control of Discord, Inc. ("Provider"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-2:

(a) A copy or image of **Server ID: 419619233622654986**, also known as "**Ryan's Underground Hangout**" (**SUBJECT DISCORD SERVER**);

(b) The contents of all chats, posts or direct messages associated with the **SUBJECT ACCOUNT (User ID: 451537312900317201**, also known as username "**ryanrocks462#8138**") from **July 1, 2016 or account creation, whichever is earlier, to the present**, including any uploaded images or video clips, stored or preserved copies of posts or direct messages associated with the account, draft messages, the date and time at which each message was sent or received or a post was made, participants in the particular chat; and the identity of the sender or receiver of each direct message;

(c) Past and current profile(s) for the **SUBJECT ACCOUNT**;

(d) All subscriber records regarding the user of the **SUBJECT ACCOUNT** and the *owner* of the **SUBJECT DISCORD SERVER**, to include full name, birth date, contact email address, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

connecting, log files, and means and source of payment (including any credit or bank account number);

(e) All past and current usernames, account passwords, and names associated with the **SUBJECT ACCOUNT**;

(f) A list of all accounts associated with the **SUBJECT ACCOUNT**, including, but limited to, any email, social media or networking, or cloud storage account;

(g) The types of service utilized associated with the **SUBJECT ACCOUNT**;

(h) Log of all voice or video chats associated with the **SUBJECT ACCOUNT**, including, but not limited to, the date/time, duration, and participants involved;

(i) All "lists" created or stored at any time by a user of the **SUBJECT ACCOUNT**, including "friend list," address books, contact and buddy lists;

(j) All stored photographs, images, or video clips associated with the **SUBJECT ACCOUNT**;

(k) A list of all Discord "servers" in which the **SUBJECT ACCOUNT** was a member or participant, from **July 1, 2016 or account creation, whichever is earlier, to the present**;

(l) All privacy and account settings;

(m) All location data associated with the **SUBJECT ACCOUNT**, including all information regarding locations where the account was accessed;

(n) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government **within 14 days** of service of this warrant.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), those violations occurring since at least October 2016 to the present, including, for each account or identifier listed on Attachment A-2, information pertaining to the following matters:

(a) Evidence of any attempt or plan to engage in computer hacking activity; access to computers or servers of Nintendo or to files, information, or data related to Nintendo products; the possession, use, or transfer of Nintendo authentication credentials, stolen property, or files, information, or data related to Nintendo or Nintendo products; research or reconnaissance about Nintendo products, release dates, or developer tools;

(b) Evidence of prior contact with law enforcement, including the Federal Bureau of Investigation (FBI);

(c) Evidence of the account user's true name, identity and use of aliases or monikers;

(d) Evidence of the account user's ownership, use, or access to other online accounts, including, but not limited to, email, social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive) accounts;

(e) Evidence of efforts to encrypt data or destroy evidence;

(f) Evidence indicating the account user's state of mind as it relates to the crime under investigation;

(g) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

(h) Any address lists or buddy/contact lists associated with the specified account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(i) All messages, documents and profile information, attachments, or other data that otherwise constitute or identify the fruits or proceeds, or the instrumentalities, of the criminal violations of Title 18, United States Code, described above.

(j) All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

(k) Any and all other log records, including IP address captures, associated with the specified account;

(l) Any records of communications between Provider, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This includes, but is not limited to, records of contacts between the subscriber and Provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

(m) All messages, documents and profile information, attachments, or other data that that identify person(s) who communicated with the account user about matters relating to the offense conduct, as described in paragraph (a), above, including records that help reveal their whereabouts. This includes, but is not limited to, an individual referred to as "anon."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-3

Apple Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following account(s):

Apple ID: 1710515926, associated with **ryanrocks462@icloud.com**

("SUBJECT ACCOUNT")

as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by Apple, Inc., an e-mail provider headquartered at One Apple Park Way, Cupertino, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-3

Items to be Seized

I. Information to be disclosed by Apple, for search:

To the extent that the information described in Attachment A-3 is within the possession, custody, or control of Apple, Inc. ("Provider"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-3:

(a) All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, methods of connecting, and means and source of payment (including any credit or bank account numbers);

(b) All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"), Subscriber Identity Modules ("SIM"), Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN"), International Mobile Subscriber Identities ("IMSI"), and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

International Mobile Station Equipment Identities ("IMEI");

(c) All stored photographs, video clips, or images;

(d) The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

(e) All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), messaging and query logs (including iMessage, SMS, and MMS messages), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find my iPhone logs, logs associated with iOS device activation and upgrades, and logs associated with web-based access of Apple services (including all associated identifiers);

(f) All records and information regarding locations where the account was accessed, including all data stored in connection with Location Services;

(g) All records pertaining to the types of service used;

(h) All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files);

(i) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government **within 14 days** of service of this warrant.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), those violations occurring since at least October 2016 to the present, including, for each account or identifier listed on Attachment A-3, information pertaining to the following matters:

(a) Evidence of any attempt or plan to engage in computer hacking activity; access to computers or servers of Nintendo or to files, information, or data related to Nintendo products; the possession, use, or transfer of Nintendo authentication credentials, stolen property, or files, information, or data related to Nintendo or Nintendo products; research or reconnaissance about Nintendo products, release dates, or developer tools;

(b) Evidence of prior contact with law enforcement, including the Federal Bureau of Investigation (FBI);

(c) Evidence of the account user's true name, identity and use of aliases or monikers;

(d) Evidence of the account user's ownership, use, or access to other online accounts, including, but not limited to, email, social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive) accounts;

(e) Evidence of efforts to encrypt data or destroy evidence;

(f) Evidence indicating the account user's state of mind as it relates to the crime under investigation;

(g) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

(h) Any address lists or buddy/contact lists associated with the specified account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(i) All messages, documents and profile information, attachments, or other data that otherwise constitute or identify the fruits or proceeds, or the instrumentalities, of the criminal violations of Title 18, United States Code, described above.

(j) All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

(k) Any and all other log records, including IP address captures, associated with the specified account;

(l) Any records of communications between Provider, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This includes, but is not limited to, records of contacts between the subscriber and Provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

(m) All messages, documents and profile information, attachments, or other data that that identify person(s) who communicated with the account user about matters relating to the offense conduct, as described in paragraph (a), above, including records that help reveal their whereabouts. This includes, but is not limited to, an individual referred to as "anon."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A-4

Google Accounts to be Searched

The electronically stored data, information and communications contained in, related to, and associated with, including all preserved data associated with the following account(s):

Account ID: 279578011651, associated with **ryanrocks562@gmail.com**

("SUBJECT ACCOUNT")

as well as all other subscriber and log records associated with each account, which are located at premises owned, maintained, controlled or operated by Google, LLC, an e-mail provider headquartered at 600 Amphitheatre Parkway, Mountain View, California.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B-4

Items to be Seized

I. Information to be disclosed by Google, for search:

To the extent that the information described in Attachment A-4 is within the possession, custody, or control of Google, LLC ("Provider"), regardless of whether such information is located within or outside of the United States, including any e-mails, records, files, logs, or information that has been deleted but is still available to Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f), the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A-4:

(a) All subscriber records associated with the specified account, including 1) names, email addresses, and screen names; 2) physical addresses; 3) records of session times and durations; 4) length of service (including start date) and types of services utilized; 5) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address such as internet protocol address, media access card addresses, or any other unique device identifiers recorded by Google in relation to the account; 6) account log files (login IP address, account activation IP address, and IP address history); 7) detailed billing records/logs; 8) means and source of payment; and 9) lists of all related accounts;

(b) Google Web & Activity content, including information and records for web browsing activity, from **July 1, 2016 to the present**;

(c) Any records for search history from **July 1, 2016 to the present**;

(d) The types of service utilized;

(e) Records (not including content) regarding any Google Drive or other cloud storage account associate with the account, to include the registration or opening date, the storage capacity, and activity log;

(f) All IP logs and other documents showing the IP address, date, and time of each

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

login to the account;

(g) All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken.

The Provider is hereby ordered to disclose the above information to the government **within 14 days** of service of this warrant.

//

//

//

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence and instrumentalities of violations of Title 18, United States Code, Sections 371 and 1349 (Conspiracy), 1028(a)(7) (Identity Theft); 1028A (Aggravated Identity Theft); 1029(a)(2) (Access Device Fraud); 1030(a)(2), (4) and (5)(A) (Computer Fraud/Hacking); and 1343 (Wire Fraud), those violations occurring since at least October 2016 to the present, including, for each account or identifier listed on Attachment A-4, information pertaining to the following matters:

(a) Evidence of any attempt or plan to engage in computer hacking activity; access to computers or servers of Nintendo or to files, information, or data related to Nintendo products; the possession, use, or transfer of Nintendo authentication credentials, stolen property, or files, information, or data related to Nintendo or Nintendo products; research or reconnaissance about Nintendo products, release dates, or developer tools;

(b) Evidence of prior contact with law enforcement, including the Federal Bureau of Investigation (FBI);

(c) Evidence of the account user's true name, identity and use of aliases or monikers;

(d) Evidence of the account user's ownership, use, or access to other online accounts, including, but not limited to, email, social media or networking (e.g., Twitter, Discord), cloud storage (e.g., Google Drive) accounts;

(e) Evidence of efforts to encrypt data or destroy evidence;

(f) Evidence indicating the account user's state of mind as it relates to the crime under investigation;

(g) All messages, documents, and profile information, attachments, or other data that serves to identify any persons who use or access the account specified, or who exercise in any way any dominion or control over the specified account;

(h) Any address lists or buddy/contact lists associated with the specified account;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

(i) All messages, documents and profile information, attachments, or other data that otherwise constitute or identify the fruits or proceeds, or the instrumentalities, of the criminal violations of Title 18, United States Code, described above.

(j) All subscriber records associated with the specified account, including name, address, local and long distance telephone connection records, or records of session times and durations, length of service (including start date) and types of service utilized, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, and means and source of payment for such service) including any credit card or bank account number;

(k) Any and all other log records, including IP address captures, associated with the specified account;

(l) Any records of communications between Provider, and any person about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users about the specified account. This includes, but is not limited to, records of contacts between the subscriber and Provider's support services, as well as records of any actions taken by the provider or subscriber as a result of the communications.

(m) All messages, documents and profile information, attachments, or other data that that identify person(s) who communicated with the account user about matters relating to the offense conduct, as described in paragraph (a), above, including records that help reveal their whereabouts. This includes, but is not limited to, an individual referred to as "anon."

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970

CERTIFICATE OF AUTHENTICITY OF DOMESTIC RECORDS PURSUANT TO FEDERAL RULES OF EVIDENCE 902(11) AND 902(13)

I, _____, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by _____, and my title is _____. I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of _____. The attached records consist of _____

_____

[GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of _____, and they were made by _____ as a regular practice; and

b. such records were generated by _____'s electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of _____ in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by _____, and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

_____ _____

Date Signature

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5200
SEATTLE, WASHINGTON 98101
(206) 553-7970